

Sicherheitsanforderung

M365 Power Automate

Deutsche Telekom Gruppe

Version	2.2
Datum	01.12.2023
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 8.03	Dokumententyp Sicherheitsanforderung
Version 2.2	Stand 01.12.2023	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.12.2023 - 30.11.2028	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung

Power Automate ist ein Dienst, mit dem automatisierte Workflows zwischen Apps und Diensten erstellt werden können, um z. B. Dateien zu synchronisieren, Benachrichtigungen zu erhalten und/oder Daten zu sammeln.

Copyright © 2023 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Data Connectors	5
3.	Logging & Detection	6
4.	Access Policies	7
5.	Templates & Flows	8

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus der Konzernrichtlinie Sicherheit (Group Security Policy). Die vorliegende Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Vorgaben der Konzernrichtlinie Sicherheit (Group Security Policy) in Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden und gelten für alle M365 Umgebungen der jeweiligen Einheit.

Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten. Sollte die Einhaltung der beschriebenen Anforderungen in individuellen Fällen nicht oder nur eingeschränkt umsetzbar sein, ist gemeinsam mit einem Sicherheits- und/oder Datenschutzexperten (entsprechend der betroffenen Anforderung) eine Risikobewertung vorzunehmen und mögliche alternative Schutzmaßnahmen abzustimmen.

2. Data Connectors

Req 1	Blockable Data Connectors müssen durch einen Approval Prozess abgenommen werden
-------	---

Vor der Verwendung der blockable Data Connectors müssen diese im Rahmen eines PSA Verfahrens beschrieben und freigegeben werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.03-1/2.2

Req 2	Externe Systeme, die per Data Connector angebunden werden, dürfen nur mit einer Authentication verwendet werden
-------	---

Werden externe Systeme, die außerhalb der eigenen Organisation liegen, mittels Data Connectors angebunden, so muss eine Authentication am externen System durchgeführt werden.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.03-2/2.2

Req 3	Nur freigegebene interne Systeme dürfen per Data Connector angebunden werden
-------	--

Interne Systeme der Organisation müssen vor einer Anbindung durch einen Data Connector im Rahmen eines PSA Verfahrens freigegeben sein.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.03-3/2.2

3. Logging & Detection

Req 4	Audit Logs & Anomalie Erkennung müssen aktiviert werden
-------	---

Im Rahmen des Betriebs der Power Apps müssen Audit Logs und die Anomalie Erkennung aktiviert und an das SIEM der Organisation angebunden werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.03-4/2.2

4. Access Policies

Req 5	Für den Zugriff auf den Common Data Service muss eine Conditional Access (CA) Policy implementiert werden
-------	---

Es dürfen nur berechnigte Personen bzw. Applikationen auf den Common Data Service zugreifen. Aus diesem Grund muss eine CA Policy erstellt und aktiviert werden die nur berechtigten Rollen und/oder Accounts Zugriff auf den Common Data Service erlaubt.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechnigte Einsichnahme oder Abgriff von Daten
- Unberechnigte Modifikation von Daten
- Unberechnigte Nutzung von Diensten oder Ressourcen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.03-5/2.2

5. Templates & Flows

Req 6	Templates dürfen in der externen Community nicht geteilt werden
-------	---

Erstellte Templates dürfen außerhalb der Organisation nicht mit anderen Personen oder Institutionen geteilt werden.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.03-6/2.2

Req 7	Flows dürfen nicht geteilt werden
-------	-----------------------------------

Erstellte Flows dürfen nicht durch die Option "Share by adding users as co-owner to flow" geteilt werden.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.03-7/2.2

Req 8	Es muss die Option "Secure Inputs / Secure Outputs" bei der Entwicklung von Flows aktiviert werden
-------	--

Während der Laufzeit eines Flows werden automatisch Logs erzeugt, die sowohl Daten als auch Metadaten enthalten. Jeder Benutzer, der Zugriff auf den Flow hat, ist in der Lage, diese per XML-Export zu extrahieren. Mit der Option "Secure Inputs / Secure Outputs" werden die im Log enthaltenen Daten sowie Metadaten verschlüsselt. Aus diesem Grund müssen erstellte Flows die Option "Secure Inputs / Secure Outputs" aktiviert haben.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Motivation: Verringerung der Wahrscheinlichkeit der Daten Exfiltration

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.03-8/2.2